

Réponses

Correction de l'épilogue

Coups de pouce :

1. Écris une équation pour chaque point qui est vraiment sur la courbe.
 2. Les inconnues sont les coefficients du polynôme.
 3. Tu peux résoudre le système d'équations en procédant par substitution, par exemple.
- Dans la lettre « Épilogue », quatre points $P_1 = (17 ; 63)$, $P_2 = (10 ; 7)$, $P_3 = (5 ; 27)$ et $P_4 = (3 ; 45)$ ont été définis.

La vérification donne :

- Pour P_1 :
 - Pour y : $13^y \equiv 13^{63} \equiv 18 \pmod{19}$
 - Pour x : $10 \times 3^{x^1} \times 13^{x^2} \equiv 10 \times 3^{17^1} \times 13^{17^2} \equiv 18 \pmod{19}$
- Pour P_2 :
 - Pour y : $13^y \equiv 13^7 \equiv 10 \pmod{19}$
 - Pour x : $10 \times 3^{x^1} \times 13^{x^2} \equiv 10 \times 3^{10^1} \times 13^{10^2} \equiv 10 \pmod{19}$
- Pour P_3 :
 - Pour y : $13^y \equiv 13^{27} \equiv 18 \pmod{19}$
 - Pour x : $10 \times 3^{x^1} \times 13^{x^2} \equiv 10 \times 3^{5^1} \times 13^{5^2} \equiv 18 \pmod{19}$

- Pour P_4 :
 - Pour y : $13^y \equiv 13^{45} \equiv 18 \pmod{19}$
 - Pour x : $10 \times 3^{x^1} \times 13^{x^2} \equiv 10 \times 3^{3^1} \times 13^{3^2} \equiv 15 \pmod{19}$

Le point à éliminer est donc P_4 .

Les trois autres points appartiennent tous à une courbe d'équation :

$$y = ax^2 + bx + s$$

Les coordonnées des points permettent d'écrire un système d'équations dont les inconnues sont les coefficients de la courbe. Le résultat obtenu en résolvant le système est $a = 1$, $b = -19$, et $s = 97$.

Le nombre $s = 97$ constitue l'ultime secret.

Détails pour la correction des lettres

- Solution de la lettre 1 (demifloat) :

Coups de pouce :

1. Chaque nombre correspond à deux caractères.
2. Connais-tu les représentations des nombres « à virgule » en informatique ? Ici, tu n'auras besoin que de seize bits par nombre.
3. Il faut lire le schéma de l'indice de bas en haut.

1129.0	36448.0	1392.0	16896.0
di	xs	ep	t

Le nombre secret est : 17.

Solution détaillée pour 1129.0 :

- Le bit de signe est 0, puisque 1129.0 est positif ou nul.
- Pour obtenir un nombre de la forme 1,..., il faut diviser 1129.0 par $2^{10} = 1024$, car $\frac{1129.0}{1024} = 1.1025390625$, donc l'exposant est 10 + 15 = 25, ce qui donne sur 5 bits 11001.
- Ensuite, $1.1025390625 - 1 = 0.1025390625$. Ce nombre doit être multiplié par 1024, donc la mantisse est 105, ce qui donne sur 10 bits 0001101001
- En concaténant les trois parties, les 16 bits sont 0110010001101001, et se décomposent en 01100100 et 01101001, qui correspondent respectivement aux caractères d et i en ASCII sur 8 bits.

Pour plus de détails, voir à la fin.

- Solution de la lettre 2 (sphinx) :

Coups de pouce :

1. Patience et longueur de temps fort plus que force ni que rage. (Jean de la Fontaine, 1668)
2. Une règle et le tableau des alphabets mélangés pourraient t'être utiles.
3. Le mot SALUTATION comporte exactement 10 lettres.

Le fait que SALUTATION se chiffre en BJJUWISMSA permet de déterminer la position des 20 barres de la machine Sphinx :

En haut : [15, 18, 7, 1, 8, 19, 14, 9, 2, 17]

En bas : [5, 12, 13, 16, 20, 6, 3, 11, 4, 10]

Ainsi le cryptogramme :

BJJUWISMSABXMRPVSQXWFRC

se déchiffre en :

SALUTATIONSOIXANTETROIS

Le nombre secret est : 63.

Pour plus de détails, voir à la fin.

• Solution de la lettre 3 (alien) :

Coups de pouce :

1. Chercher à décrypter est inutile, mieux vaut observer.
2. Cherche ce qui se ressemble.
3. Deux messages contenant un « mot » en commun font partie du même ensemble.

Le groupe de la première phrase est écrit en gras

et les mots en rouge permettent relier ces phrases.

JXMUSCC YLC BMFLMGO YZZJN ZB **CGWOWN KYVGB**
VL FEL SIYBL **EROXA EUVSD**
CGWOWN **BDR HEIOE OMSBA WI**
WAMRBBI BHKFETL MN RR SY PAKZAC
EYHPR AECBN GUNLLU
NW IGEL KDYUNQN **ORK NIX**
TVLDAHB JHKKKZ RQJBPH FPAW GUNLLU XH YAUGMZZ
SY TEIW PVRPJ TR UIIKDUJ SWBZHQL QN
KTNFCEZ HQXYAKW IK THIHGMG WTB PVRPJ DBMH
YGX PMKV SNIETY EROXA XGS XHNCM ZMLLDS
GNTVW ARS ZJSU YAUGMZZ EROXA
UFJWJN KPYGDX KTNFCEZ ZGT UGHLJNC
PVRPJ NXJMA TGO
BDR UJUC NW LRV
LM HBZYYR EYHPR
FUK ORK EROXA ZU IOPHJA LCX DQLF WMK

La liste ci-dessus contient en tout 16 phrase, dont 11 dans le groupe de la première phrase, donc le chiffre à retenir est : 1

Le groupe de la première phrase est écrit en gras

et les mots en rouge permettent relier ces phrases.

DAZSXB TP DW WCGHN HVWCB GDR

ULV CS DIUXQ

TH OGH OEABT FIXKHH CS LBMHDE RSGU HKOEW

TIZGV XAU PXTUQJ VJRD YXF ZXDEVRX IJEDGVU

LBMHDE FYAG US FVOTA CO MCRXTOI

IZGORI CYUDRF IXQIP XZRX LBMHDE NGWMIF DSFBC

DJXLK YHCTXVP XYL CPO YBLYJ HVJLUNU CC ERGM

GDR **CYQFK PTVQNPX**

CYQFK ORPI DNP YLCXEMD XKJK IXLS IO ZXDEVRX

WVOTUY YXF KEWOSW

IFEQSMP YHWMR LBMHDE SPTHAWI

NZWFJPK LRLANNH AONOR VGZWYG LZLVPF TCHAOC UTWV

XYL XINGOBL BTZCKAC

GRX PMWY OWKWU AONOR DIUXQ MOP HSFPWW MAVLZG

CPO XJKFV TLYLJJV ZEXL

RFDVBZG BTZCKAC NONMV RJSCMP

BRSBT JWWFMZA OWLHCEE LRLANNH JRFR RP ZE LTM

YBDPAZ CPO LSJNJU QSBFTKX WVOTUY JZDNXL ZCLT

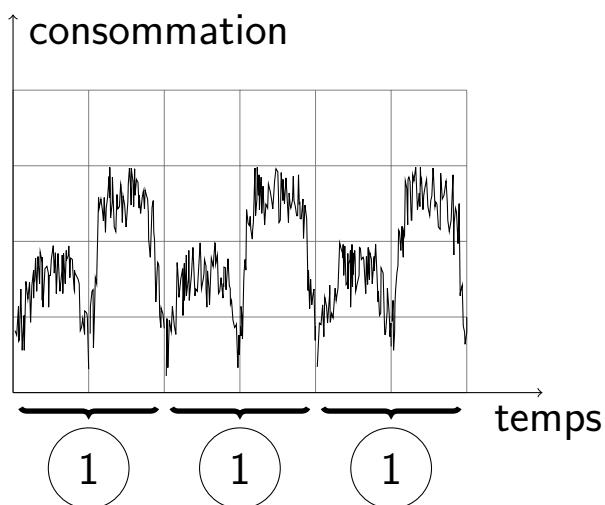
La liste ci-dessus contient en tout 18 phrase, dont 10 dans le groupe de la première phrase, donc le chiffre à retenir est : 0

Finalement, le nombre secret est : 10.

- Solution de la lettre 4 (canalauxRSA) :

Coups de pouce :

1. Vérifie l'ordre dans lequel les bits de la clé sont utilisés.
2. La solution est dans les motifs.
3. Analyse les pics de consommation : soit un carré seulement (bit égal à 0) ; soit un carré suivi d'une multiplication (bit égal à 1).

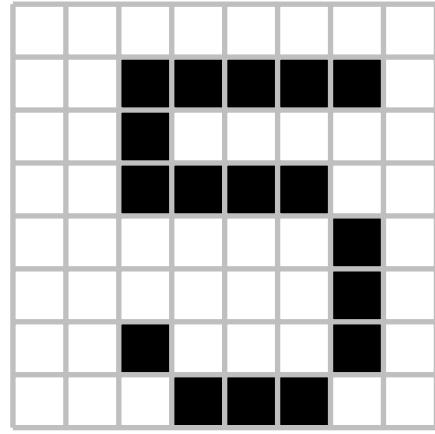
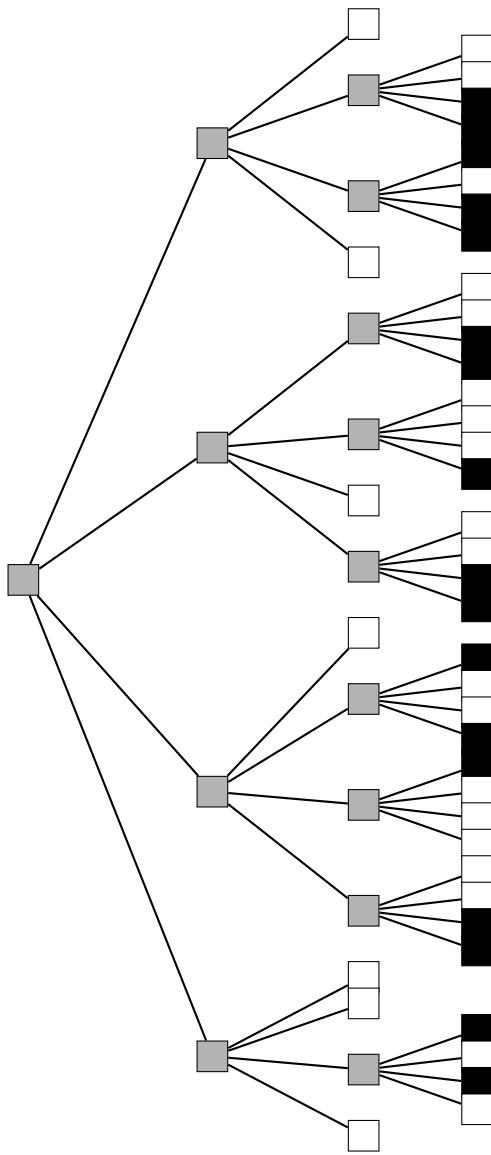


En binaire : 111

En decimal : 7

Le nombre secret est : 7.

- Solution de la lettre 5 (quadtree) :



Le nombre secret est : 5.

- Solution de la lettre 6 (dhgrille) :

Dans le premier cas, Alice part de la case $(-7 ; 10)$ et arrive sur la case $(0 ; 19)$ en suivant son chemin secret. Il est inutile de le connaître entièrement pour calculer qu'elle se déplace du vecteur $(0 ; 19) - (-7 ; 10) = (7 ; 9)$. De même, Bob se déplace du vecteur $(-1 ; 6) - (-7 ; 10) = (6 ; -4)$. Pour trouver la case secrète, il suffit d'ajouter le vecteur du déplacement d'Alice à la case de Bob, ou de façon équivalente, le vecteur

du déplacement de Bob à la case d'Alice. Ainsi, les coordonnées de la première case secrète sont : $(0 ; 19) + (6 ; -4) = (-1 ; 6) + (7 ; 9) = (6 ; 15)$.

Les coordonnées de la seconde case secrète se calculent de la même façon : $(-17; -8) + (9; 16) - (-11; -2) = (9; 16) + (-17; -8) - (-11; -2) = (3 ; 10)$.

Cases secrètes : (6 ; 15) et (3 ; 10)

Les quatre nombres a , b , c et d ainsi obtenus servent de clé de déchiffrement de Hill pour trouver le nombre secret de cette lettre :

GZUFMTFAT

VINGTSEPT

Le nombre secret est : 27.

- Solution de la lettre 7 (bandelettes avec [2, 6, 4, 9, 12, 8, 13, 7, 1, 11, 0, 10, 5, 3]) :

L	E		N	O	M	B	R	E		S	E	C	R
E	T	D	E		C	E	T	T	E		L		E
T	T	R	E	E	S	T		T	R	O	I	S	
,	O	B	T	E	N	U		E	N		R	E	
O	R	D	O	N	N	A	N	T	L	E	S		
B	A	N	D	E	L	E	T	T	E	S	.		I
L	S	E	R	A		U	T	I	L	E			P
A	R	L	A	S	U	I	T	E	.		D		
A	N	S	L	E	P	I	L	O	G	U	E		

Le nombre secret est : 3.

- Solution de la lettre 8 (résistance) :



Les deux bandes de gauche correspondent aux deux chiffres d'un nombre entre 10 et 99 et la bande de droite correspond à l'exposant de la puissance de dix par laquelle il faut le multiplier pour trouver la résistance en ohms.

Le code couleurs est le suivant :

Black	Brown	Red	Orange	Yellow	Green	Blue	Magenta	Grey	White	Gold	Silver
0	1	2	3	4	5	6	7	8	9	-1	-2

Le calcul est :

$$45 \times 10^0 = 45$$

Le nombre secret est : 45.

Détails de la solution de la lettre 1 (demifloat)

Pour la suite de la solution, les calculs sont présentés sous forme de tableaux :

Nombre	36448.0	
Signe	≥ 0	Sur 1 bit 0
Exposant	$\frac{36448.0}{2^{15}} = 1.1123046875$ $15 + 15 = 30$	Sur 5 bits 11110
Mantisse	$(1.1123046875 - 1) \times 1024$ $= 115$	Sur 10 bits 0001110011
Regroupement sur 16 bits	0111100001110011	
Codes ASCII sur 8 bits	01111000	01110011
Caractères	x	s

Nombre	1392.0	
Signe	≥ 0	Sur 1 bit 0
Exposant	$\frac{1392.0}{2^{10}} = 1.359375$ $10 + 15 = 25$	Sur 5 bits 11001
Mantisse	$(1.359375 - 1) \times 1024$ $= 368$	Sur 10 bits 0101110000
Regroupement sur 16 bits	0110010101110000	
Codes ASCII sur 8 bits	01100101	01110000
Caractères	e	p

Nombre	16896.0	
Signe	≥ 0	Sur 1 bit 0
Exposant	$\frac{16896.0}{2^{14}} = 1.03125$ $14 + 15 = 29$	Sur 5 bits 11101
Mantisse	$(1.03125 - 1) \times 1024$ $= 32$	Sur 10 bits 0000100000
Regroupement sur 16 bits	0111010000100000	
Codes ASCII sur 8 bits	01110100	00100000
Caractères	t	espace

Détails de la solution de la lettre 2 (sphinx)

Voici les positions de la machine pour ce message :

15	L	K	J	I	H	G	F	E	D	C	B	18	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B																								
19	S	R	Q	P	O	N	M	L	K	J	I	17	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B																							
2	C	D	E	F	G	H	I	J	K	L	M	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B																								
10	V	W	X	Y	Z	A	B	C	D	E	F	18	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B																							
4	Z	Y	X	W	V	U	T	S	R	Q	P	5	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B																					
10	V	W	X	Y	Z	A	B	C	D	E	F	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B																				
12	5	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	10	4	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	
13	12	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	10	4	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	
16	13	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	10	4	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	
17	16	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	10	4	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	
15	17	16	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	10	4	1	8	14	9	19	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B

